CERTIFICATION UNDER 37 CFR 1.8

I hereby certify that this document is being deposited with the United States Postal Service on this date Aug 4, 2004, in an envelope as FIRST CLASS MAIL with sufficient postage addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Florence Twaddle
(Type or print name of person mailing paper)

Florence Twaddle
(Signature of person mailing paper)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Jakobsson et al.	:	
Serial No.: 09/487,946	:	Group Art Unit: 2132
Filed: 01/19/2000	:	Examiner: Kim, Jung W.
Title: NON MALLEABLE ENCRYPTION METHOD AND APPARATUS USING KEY-ENCRYPTION KEYS AND DIGITAL SIGNATURE	:	

BRIEF ON APPEAL (INCLUDES APPENDIX OF CLAIMS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following appeal brief is submitted pursuant the appeal, the notice of appeal being filed on August 4, 2004, with this brief, from the action of the primary examiner dated July 21, 2004, in the above identified application. An authorization to charge a credit card for $660.00 for filing a notice of appeal and for filing this brief in support of the appeal for a large entity is included with this brief.

I.STATUS OF CLAIMS

Claims 1-2, 5-11, and 13-18 are pending in the application. The final form of these claims is enclosed as an appendix to this appeal brief. Claims 3-4 and 12 were cancelled.

II. STATEMENT IDENTIFYING "REAL PARTY IN INTEREST"

The real party in interest in this matter is assignee Lucent Technologies, Inc., a corporation of the State of Delaware, having an office at 600 Mountain Avenue, Murray Hill, New Jersey, 07974-0636.

III.STATEMENT IDENTIFYING RELATED APPEALS AND INTERFERENCES

There are no other current appeals and there are no current interferences related to this matter.

IV.COPIES OF APPEAL PAPERS

One original and three copies of the appeal brief and appendix of final claims and all accompanying papers are enclosed.

V.APPENDIX OF CLAIMS INVOLVED IN FINAL FORM

An appendix of all the claims pending in the case in their final form is attached to the brief. (Three copies and one original of the appendix are attached to the corresponding three copies and one original of the brief).

VI. STATUS OF AMENDMENTS

The present application, serial number 09/487,946 was filed on January 19, 2000. The present application as originally filed, included eight claims. In a first office action dated October 27, 2003, the examiner rejected (A) claims 3-4 under 35 U.S.C. 112, (B) claims 1-5 under 35 U.S.C. 103 based on Schneier, Applied Cryptography 2nd Edition (hereinafter "Schneier"), and (C) and claims 6-8 under 35 U.S.C. 103 based on Schneier in view of alleged admitted prior art in applicant's specification.

The applicant amended claims 1, 3, 4, 6, and 8, and added claims 9-14 in an amendment dated November 12, 2003.

In a subsequent office action, dated January 15, 2004, the examiner rejected (1) claims 1-5 and 9-14 under 35 U.S.C. 103 based on Schneier in view of Deo, U.S. Patent No. 5,721,781 (hereinafter "Deo") and (2) claims 6-8 under 35 U.S.C. 103 based on Schneier in view of Deo and further in view of alleged admitted prior art in applicant's specification.

The applicant next filed a notice of appeal and arguments asserting the allowability of claims 1-14 on January 29, 2004. The notice of appeal was received by the United States Patent and Trademark Office on February 2, 2004.

The examiner filed a response on March 10, 2004 rejecting the applicant's arguments.

The applicant filed a request for continued examination on March 23, 2004 and an amendment, which amended claims 1, 6, 8, and 11 and cancelled claims 3, 4, and 12.

In a subsequent office action, dated April 28, 2004, the examiner rejected (i) claims 1-2, 5-11, and 13-14 under 35 U.S.C. 112, first paragraph and (ii) claims 1, 6, 8, and 11 under 35 U.S.C. 112, second paragraph.

The applicant next filed an amendment dated May 17, 2004, which amended claims 1, 2, 5, 6, 8, 11, 13, and 14 and added claims 15-18.

In a subsequent office action, dated July 21, 2004, the examiner rejected (A) claims 1, 2, 5, 9-11, 13-14, 15, and 18 under 35 U.S.C. 103(a) based on Schneier and Deo and (B) claims 6, 7, 8, 16, and 17 under 35 U.S.C 103(a) based on Schneier and Deo and further in view of alleged admitted prior art.

Claims 1-2, 5-11, 13-18 are now pending in the case. The applicant is filing a notice of appeal regarding the July 21, 2004 office action with this brief on August 4, 2004.

VII. SUMMARY OF INVENTION

Claim 1 of the present application specifies:

> A method comprising the steps of:
>
> encrypting a data message m at a transmitter processor using a primary transmitter secret key z, wherein z is known to the transmitter processor but not to a receiver processor, to form a quantity E;
>
> preparing a quadruplet (a_{new}, b_{new},s_{new}, E) at the transmitter processor where:
>
> $a_{new} = z^{*} y^{c}$ modulo p ;
>
> $b_{new} = g^{c}$modulo p;
>
> s_{new} = signature $_{c}(a_{new}, b_{new}, E)$;
>
> where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;
>
> wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};
>
> transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;
>
> verifying the signature s_{new} at the receiver processor;
>
> decrypting a_{new} and b_{new} at the receiver processor by using the receiver secret key x to get the primary transmitter secret key z;
>
> using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m at the receiver processor.

Claim 1 specifies a method including using a primary transmitter secret key z to encrypt a data message m to form a quantity (or encryption) E. Claim 1 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. The quantities a_{new} and b_{new} are defined in the claim and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of z or a ciphertext representing z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. The method also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method also includes using the primary transmitter secret key z to decrypt the quantity E and to thereby obtain the message m at the receiver processor.

Claims 2, 5, 9, 10, and 15 are dependent on claim 1 and provide one or more further limitations.

Claim 6 of the present application specifies:

6. A method comprising the steps of:

creating a primary transmitter key z at a transmitter processor wherein the primary transmitter key is known to the transmitter processor but not to a receiver processor;

creating a secondary transmitter key z' at the transmitter processor wherein the secondary transmitter key is known to the transmitter processor but not to the receiver processor, wherein the secondary transmitter key z' is a function of z;

encrypting a data message m , at the transmitter processor, using the secondary transmitter secret key z' to form a quantity E;

preparing a quadruplet (a_{new}, b_{new},s_{new}, E) at the transmitter processor, where:

$a_{new} = z^{*} y^{c}$ modulo p ;
$b_{new} = g^{c}$ modulo p;
s_{new} = signature $_{c}(a_{new}, b_{new}, E)$;

where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at the receiver processor;

decrypting a_{new} and b_{new} , at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

Claim 6 specifies a method including using a secondary transmitter secret key z' to encrypt a data message m to form a quantity (or encryption) E. Claim 6 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. The quantities a_{new} and b_{new} are defined in the claim and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of the primary transmitter key z or a ciphertext of z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. The method also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method also includes modifying the primary transmitter secret key z to get the secondary transmitter key z' and using z' to decrypt the quantity E and to thereby obtain the message m at the receiver processor.

Claims 7 and 16 are dependent on claim 6 and provide one or more further limitations. -

Claim 8 of the present application specifies:

> 8.A method comprising the steps of:
> creating a primary transmitter key z at a transmitter processor;
> creating a secondary transmitter key z' which is a function of z, at the transmitter processor;
> providing a plurality of portion keys which are derived from the secondary transmitter key z', at the transmitter processor;
> encrypting a data message m, at the transmitter processor, using the plurality of portion keys to form a quantity E;
> preparing a quadruplet (a_{new}, b_{new},s_{new}, E). at the transmitter processor, where:
>
> $a_{new} = z^{*}y^{c}$ modulo p ;
>
> $b_{new} = g^{c}$modulo p;
>
> s_{new} = signature $_{c}(a_{new},b_{new},E)$;
>
> where y = g^{x} modulo p, c is a random number, x is a receiver secret key of a receiver processor, and the parameters g, x, and p are picked using a known encryption method;
> wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};
> transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;
> verifying the signature s_{new} at the receiver processor;
> decrypting a_{new} and b_{new}, at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;
> modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to determine the plurality of portion keys and using the plurality of portion keys to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

Claim 8 specifies a method including using a plurality of portion keys, which are derived from a secondary transmitter secret key z', to encrypt a data message m to form a quantity (or encryption) E. The secondary transmitter secret key z' is a function of a primary transmitter key z. Claim 8 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. The quantities a_{new} and b_{new} are defined in the claim and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of the primary transmitter key z or a ciphertext of z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. The method also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method also includes modifying the primary transmitter secret key z to get the secondary transmitter key z', using the secondary transmitter key z' to get the portion keys, and using the portion keys to decrypt the quantity E and to thereby obtain the message m at the receiver processor.

Claim 17 is dependent on claim 8 and provides one or more further limitations.

Claim 11 of the present application specifies:

11. An apparatus comprising
a transmitter processor;
wherein the transmitter processor
encrypts a data message m using a primary transmitter secret key z, known to the transmitter processor but not known to a receiver processor, to form a quantity E; and
prepares a quadruplet (a_{new}, b_{new},s_{new}, E) where:
$a_{new} = z^{*} y^{c}$ modulo p ;
$b_{new} = g^{c}$ modulo p;
s_{new} = signature $_{c}$(a_{new},b_{new},E);

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method; and

wherein s_{new} is a signature, and wherein the transmitter processor determines s_{new} by using the same random number c that was used to determine a_{new} and b_{new}.

Claim 11 specifies an apparatus including a transmitter processor. The transmitter processor encrypts a data message m using a primary transmitter key z to form a quantity E. The transmitter processor also prepares a quadruplet (a_{new}, b_{new},s_{new}, E) where a_{new} and b_{new} are defined in the claim and are functions of a random number c. The signature s_{new} is a function of a_{new}, b_{new}, and E and of the same random number c.

Claims 13, 14, and 18 are dependent on claim 11 and also include one or more further limitations.

VIII. ISSUES – REJECTIONS BY EXAMINER

The remaining issues in the case are as follows:

(A) Were claims 1, 2, 5, 9-11, 13, 14, 15, and 18 properly rejected under 35 U.S.C. 103(a) based on Schneier in view of Deo?; and

(B) Were claims 6, 7, 8, 16, and 17 properly rejected under 35 U.S.C. 103(a) based on Schneier in view of Deo and further in view of alleged admitted prior art ?

IX. THE REFERENCES

The following references are relied on by the Examiner in the rejection of the office action of July 21, 2004, which is currently being appealed:

1. Schneier, Applied Cryptography 2nd Edition;
2. Deo, U.S. Patent No. 5,721,781 and
3. Alleged admitted prior art in specification of current application.

X. BRIEF DESCRIPTION OF THE REFERENCES

1. Schneier, Applied Cryptography 2nd Edition (hereinafter "Schneier")

Schneier discloses various general aspects of applied cryptography. Schneier does not disclose preparing a quadruplet as specified in independent claims 1, 6, 8, and 11 of the present application. Schneier does not disclose transmitting a quadruplet as specified in independent claims 1, 6, and 8 of the present application. Schneier does not disclose transmitting in a quadruplet both an encryption of a data message (E in the present application) and an encryption or ciphertext (a_{new} and b_{new} of the present application) of the key (z) which was used to encrypt the data message as specified in claim 1 of the present application. Although the examiner refers to various pages of Schneier, including pages 478, 513-515, in support of the examiner's rejections, none of the Schneier examples referred to disclose transmitting both an encrypted data message along with an encryption of the key used to the encrypt the data message.

In addition, the examiner admits that (a) "...Schneier does not specify the step of generating a signature based on the triplet a(new), b(new), and E." (examiner's 7/21/04 office action, pg. 4, lns. 9-10); (b) "... Schneier is silent on the matter of the same random number c being used in the key encryption step and in the signature step." (examiner's 7/21/04 office action, pg. 4, lns. 20-22); (c) with regards to claims 6, 7, 8, 16, and 17 of the present application, the examiner states that "Schneier is silent on the matter of defining 2 private transmitter keys z and z' where the z'=f(z) for some function f() and z' is the key which encrypts and decrypts the message M." (examiner's 7/21/04 office action, pg. 8, lns. 5-7); and (d) with regards to claim 5 of the present application "...Schneier is silent on the matter of defining a function to determine the value of z." (examiner's 7/21/04 office action, pg. 6, lns. 5-6).

2. Deo, U.S. Patent No. 5,721,781

Deo generally discloses various encryption and decryption techniques. Deo does not disclose preparing a quadruplet as specified in independent claims 1, 6, 8, and 11 of the present application. Deo does not disclose transmitting a quadruplet as specified in independent claims 1, 6, and 8 of the present application. Deo does not disclose transmitting in a quadruplet both an encryption of a data message (E in the present application) and an encryption or ciphertext (a_{new} and b_{new} of the present application) of the key (z) which was used to encrypt the data message as specified in claim 1 of the present application. Deo does not disclose generating a signature based on a triplet a_{new}, b_{new}, and E as in various claims of the present application. Deo does not disclose using the same random number in an encryption step and in a signature step. Deo does not disclose providing two private transmitter keys z and z' where the z'=f(z) for some function f() and z' is the key which encrypts and decrypts the message M.

3. Alleged Admitted prior art in present application

The examiner asserts that there is a statement in the present application regarding "truncation" which would make it obvious to define a second private transmitter key z'. (Examiner's 7/21/04 office action, referring to present application, pg. 12, ln. 14- pg. 13, ln. 3) The applicant respectfully asserts that the examiner is incorrect. It respectfully would not be obvious to define a second private transmitter key z' merely based on the fact that a general function such as "truncation", may be known.

XI. ARGUMENT

A. Point I – Claims 1, 2, 5, 9-11, 13-15, and 18 should not have been rejected under 35 U.S.C. 103(a) based on Schneier in view of Deo

The examiner has rejected claims 1, 2, 5, 9-11, 13-15, and 18 under 35 U.S.C. 103(a) based on Schneier in view of Deo. The examiner's rejections are respectfully submitted to be incorrect. The rejection of claim 1 and its dependents does not stand or fall with the rejection of claim 11 and its dependents. Claim 1 and its dependents have one or more limitations which are different from and/or which are not shown in claim 11 and its dependents and which are not disclosed or suggested by either Schneier or Deo, as will be described below. Claim 11 and its dependents have one or more limitations which are different from and/or which are not shown in claim 1 and its dependents and which are not disclosed or suggested by either Schneier or Deo, as will be described below.

i. Claim 1 and dependents

Claim 1 of the present application specifies a method including using a primary transmitter secret key z to encrypt a data message m to form a quantity (or encryption) E. Claim 1 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. Neither Schneier nor Deo discloses or suggests preparing or transmitting such a quadruplet.

The quantities a_{new} and b_{new} are defined in claim 1 of the present invention and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of z or a ciphertext representing z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. Neither Schneier nor Deo discloses or suggests using the same random number c for both a signature s_{new} and the quantities a_{new} and b_{new}.

The method of claim 1 of the present invention also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method also includes using the primary transmitter secret key z to decrypt the quantity E and to thereby obtain the message m at the receiver processor.

Neither Schneier nor Deo discloses transmitting in a quadruplet both an encryption of a data message (E in the present application) and an encryption or ciphertext (a_{new} and b_{new} of the present application) of the key (z) which was used to encrypt the data message as specified in claim 1 of the present application. Although the examiner refers to various pages of Schneier, including pages 478, 513-515, in support of the examiner's rejections, none of the examples referred to disclose transmitting both an encrypted data message along with an encryption of the key used to the encrypt the data message.

In addition, the examiner admits that (a) "...Schneier does not specify the step of generating a signature based on the triplet a(new), b(new), and E." (examiner's 7/21/04 office action, pg. 4, lns. 9-10); and (b) "... Schneier is silent on the matter of the same random number c being used in the key encryption step and in the signature step." (examiner's 7/21/04 office action, pg. 4, lns. 20-22).

Respectfully, the examiner comes up with many hindsight explanations for why the examiner feels it would be obvious to supply various limitations which are missing from Schneier or Deo. (Examiner's 7/21/04 office action, pgs. 3-5). However, these hindsight explanations are not in any way suggested by the references themselves. A suggestion is required.

Claim 1 is submitted to be allowable for at least the above reasons. Claims 2, 5, 9, 10, and 15 are dependent on claim 1 and are submitted to be allowable for at least the same reasons. In addition, with regards to claim 5 of the present application "...Schneier is silent on the matter of defining a function to determine the value of z." (examiner's 7/21/04 office action, pg. 6, lns. 5-6). The examiner provides no suggestion in the references for providing further limitations of claim 5 of the present application. Claim 5 for these additional reasons is respectfully submitted to not necessarily stand or fall with claim 1 or its other dependents.

ii. Claim 11 and dependents

Claim 11 specifies an apparatus including a transmitter processor. The transmitter processor encrypts a data message m using a primary transmitter key z to form a quantity E. The transmitter processor also prepares a quadruplet (a_{new}, b_{new},s_{new}, E) where a_{new} and b_{new} are defined in the claim and are functions of a random number c. The signature s_{new} is a function of a_{new}, b_{new}, and E and of the same random number c.

Neither Schneier nor Deo discloses or suggests preparing a quadruplet as specified in claim 11 of the present application. Neither Schneier nor Deo discloses or suggests using the same random number c for both a signature s_{new} and the quantities a_{new} and b_{new}.

Claim 11 is submitted to be allowable for at least the foregoing reasons. Claims 13, 14, and 18 are dependent on claim 11 and are also submitted to be allowable for at least the above reasons.

B. **Point II – Claims 6, 7, 8, 16, and 17 should not have been rejected under 35 U.S.C. 103(a) based on Schneier in view of Deo and further in view of alleged admitted prior art**

The examiner has rejected claims 6, 7, 8, 16, and 17 under 35 U.S.C. 103(a) based on Schneier in view of Deo and further in view of alleged admitted prior art. The examiner's rejections are respectfully submitted to be incorrect. The rejection of claim 6 and its dependents does not stand or fall with the rejection of claim 8 and its dependents. Claim 6 and its dependents have one or more limitations which are different from and/or which are not shown in claim 8 and its dependents and which are not disclosed or suggested by either Schneier, Deo, or the alleged admitted prior art, as will be described below. Claim 8 and its dependents have one or more limitations which are different from and/or which are not shown in claim 6 and its dependents and which are not disclosed or suggested by either Schneier, Deo, or the alleged admitted prior art as will be described below.

i. Claim 6 and dependents

Claim 6 specifies a method including using a secondary transmitter secret key z' to encrypt a data message m to form a quantity (or encryption) E. Claim 6 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests preparing or transmitting such a quadruplet.

The quantities a_{new} and b_{new} are defined in claim 6 of the present invention and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of the primary transmitter key z or a ciphertext of z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests using the same random number c for both an encryption and a signature process. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests having a signature which is a function of a_{new}, b_{new}, and E as defined in claim 6 of the present invention.

The method of claim 6 also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method also includes modifying the primary transmitter secret key z to get the secondary transmitter key z' and using z' to decrypt the quantity E and to thereby obtain the message m at the receiver processor. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests decrypting to get a primary transmitter secret key, then modifying to get a secondary transmitter secret key, and then using the secondary transmitter secret key to decrypt a quantity E as defined in claim 6 of the present invention.

Claim 6 is submitted to be allowable for at least the foregoing reasons. Claims 7 and 16 are dependent on claim 6 and are submitted to be allowable for at least the same reasons.

ii. Claim 8 and its dependents

Claim 8 specifies a method including using a plurality of portion keys, which are derived from a secondary transmitter secret key z', to encrypt a data message m to form a quantity (or encryption) E. The secondary transmitter secret key z' is a function of a primary transmitter key z. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests using a plurality of portion keys, which are derived from a secondary transmitter secret key to encrypt a data message m to form a quantity E, where the secondary transmitter secret key is a function of a primary transmitter secret key.

Claim 8 also specifies preparing a quadruplet comprised of (a_{new}, b_{new}, s_{new}, E) and transmitting that quadruplet to a receiver processor. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests preparing or transmitting such a quadruplet.

The quantities a_{new} and b_{new} are defined in claim 8 of the present invention and each is a function of a random number c. The quantities a_{new} and b_{new} can be thought of as an encryption of the primary transmitter key z or a ciphertext of z. The quantity s_{new} is a signature which is a function of a_{new}, b_{new}, and E and which is determined using the same random number c that was used to determine a_{new} and b_{new}. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests using the same random number c for both an encryption and a signature process. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests having a signature which is a function of a_{new}, b_{new}, and E as defined in claim 8 of the present invention.

The method of claim 8 of the present invention also includes verifying the signature s_{new} at the receiver processor, decrypting a_{new} and b_{new} at the receiver processor by using a receiver secret key x to get the primary transmitter secret key z. The method of claim 8 of the present invention also includes modifying the primary transmitter secret key z to get the secondary transmitter key z', using the secondary transmitter key z' to get the portion keys, and using the portion keys to decrypt the quantity E and thereby obtain the message m at the receiver processor. Neither Schneier nor Deo nor the alleged admitted prior art discloses or suggests decrypting to get a primary transmitter secret key, modifying the primary transmitter secret key to get a secondary transmitter secret key, using the secondary transmitter secret key to get portion keys, and then using the portion keys to decrypt a quantity E as define in claim 8 of the present invention.

Claim 8 is submitted to be allowable for at least the foregoing reasons. Claim 17 is dependent on claim 8 and is submitted to be allowable for at least the same reasons.

XII. CONCLUSION

In view of the foregoing, the remaining claims (claims 1-2, 5-11, and 13-18) in the case are considered to be in a condition for allowance. Favorable reconsideration of this application, is respectfully requested.

DATED: 8/4/04

Respectfully submitted,
Walter J. Tencza Jr.
Reg. No. 35,708
Suite 3
10 Station Place
Metuchen, N.J. 08840
(732) 549 – 3007
Fax: (732) 549 - 8486

APPENDIX OF FINAL FORM OF CLAIMS INVOLVED IN APPEAL

1. A method comprising the steps of:

encrypting a data message m at a transmitter processor using a primary transmitter secret key z, wherein z is known to the transmitter processor but not to a receiver processor, to form a quantity E;

preparing a quadruplet (a_{new}, b_{new},s_{new}, E) at the transmitter processor where:

$a_{new} = z^{*} y^{c}$ modulo p ;
$b_{new} = g^{c}$modulo p;
s_{new} = signature $_{c}(a_{new},b_{new},E)$;

where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at the receiver processor;

decrypting a_{new} and b_{new} at the receiver processor by using the receiver secret key x to get the primary transmitter secret key z;

using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m at the receiver processor.

2. The method of claim 1 and wherein:

the step of decrypting a_{new} and b_{new} at the receiver processor using the receiver secret key x to get the primary transmitter secret key z is comprised of computing $z = a_{new}/b_{new}^{x}$.

5. The method of claim 1 wherein:

the primary transmitter secret key z is determined at the transmitter processor from the formula of $z = g^{\Upsilon}$ modulo p, where Υ is a random value chosen from the set [0..q], where q is a value picked using a known encryption method.

6. A method comprising the steps of:

creating a primary transmitter key z at a transmitter processor wherein the primary transmitter key is known to the transmitter processor but not to a receiver processor;

creating a secondary transmitter key z' at the transmitter processor wherein the secondary transmitter key is known to the transmitter processor but not to the receiver processor, wherein the secondary transmitter key z' is a function of z;

encrypting a data message m , at the transmitter processor, using the secondary transmitter secret key z' to form a quantity E;

preparing a quadruplet (a_{new}, b_{new},s_{new}, E) at the transmitter processor, where:

$a_{new} = z^{*} y^{c}$ modulo p ;
$b_{new} = g^{c}$modulo p;
s_{new} = signature $_{c}(a_{new}, b_{new}, E)$;

where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at the receiver processor;

decrypting a_{new} and b_{new} , at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

7.The method of claim 6 and wherein:

the primary transmitter key z is provided which is not of the format used for producing the ciphertext E;

the secondary transmitter key z' is computed as a function of z, where the function is an arbitrary function.

8.A method comprising the steps of:

creating a primary transmitter key z at a transmitter processor;

creating a secondary transmitter key z' which is a function of z, at the transmitter processor;

providing a plurality of portion keys which are derived from the secondary transmitter key z', at the transmitter processor;

encrypting a data message m, at the transmitter processor, using the plurality of portion keys to form a quantity E;

preparing a quadruplet (a_{new}, b_{new},s_{new}, E). at the transmitter processor, where:

$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$ modulo p;
s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key of a receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new},s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at a the receiver processor;

decrypting a_{new} and b_{new}, at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to determine the plurality of portion keys and using the plurality of portion keys to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

9.The method of claim 1 wherein

the signature s_{new} is determined by using a Schnorr signature method.

10. The method of claim 1 wherein

the signature s_{new} is determined using a Digital Signature Standard.

11. An apparatus comprising

a transmitter processor;

wherein the transmitter processor

encrypts a data message m using a primary transmitter secret key z, known to the transmitter processor but not known to a receiver processor, to form a quantity E; and

prepares a quadruplet (a_{new}, b_{new},s_{new}, E) where:

$a_{new} = z^{*} y^{c}$ modulo p ;
$b_{new} = g^{c}$modulo p;
s_{new} = signature $_{c}(a_{new},b_{new},E)$;

where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method; and

wherein s_{new} is a signature, and wherein the transmitter processor determines s_{new} by using the same random number c that was used to determine a_{new} and b_{new}.

13.The apparatus of claim 11 wherein

the transmitter processor uses a Schnorr signature method to determine s_{new}.

14. The apparatus of claim 11 wherein

the transmitter processor uses a Digital Signature Standard to determine s_{new}.

15. The method of claim 1 wherein

El Gamal encryption is used for the encrypting steps.

16.The method of claim 6 wherein

El Gamal encryption is used for the encrypting steps.

17.The method of claim 8 wherein

El Gamal encryption is used for the encrypting steps.

18.The apparatus of claim 11 wherein

El Gamal encryption is used for encrypting.

DATED: 8/4/04

Respectfully submitted,

Walter J. Tencza Jr.

Reg. No. 35,708
Suite 3
10 Station Place
Metuchen, N.J. 08840
(732) 549-3007
Fax (732) 549-8486